

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-030053

(43)Date of publication of application : 31.01.2003

(51)Int.Cl.

G06F 12/14  
G06F 3/06  
G06F 12/00

(21)Application number : 2001-213642

(22)Date of filing : 13.07.2001

(71)Applicant : HITACHI LTD

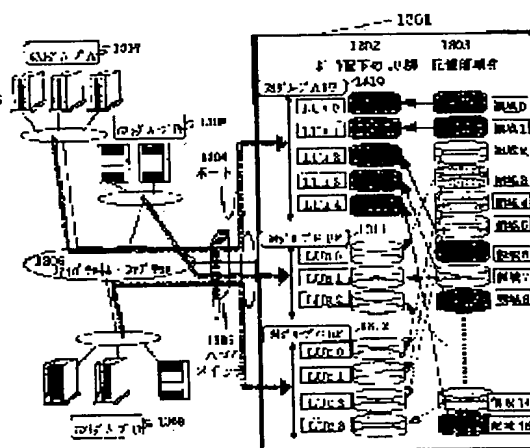
(72)Inventor : ITO RYUSUKE  
OKAMI YOSHINORI  
UCHIUMI KATSUHIRO  
IGARASHI YOSHINORI  
HORI KOICHI

## (54) STORAGE SUBSYSTEM HAVING SECURITY FUNCTION FOR EACH LOGICAL UNIT

## (57)Abstract:

PROBLEM TO BE SOLVED: To solve the problem that security by every logical unit is not realized while efficiently using system resources by the conventional LUN(logical unit number) security function in a storage subsystem to which access from various computers is expected.

SOLUTION: The storage subsystem is provided with a table to regulate an information WWN(world wide name) to uniquely identify a computer, an information GID(group ID) to identify a group to which the computer belongs and a logical unit number LUN in the storage subsystem to which access from a host computer is permitted by an operating method optional to a user and to disclose the logical unit number to a host computer. Propriety of access to the logical unit in the storage subsystem is determined by unit of group to a group of computers optionally grouped by the user by using a management table in the storage subsystem.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-30053

(P2003-30053A)

(43) 公開日 平成15年1月31日 (2003.1.31)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)	
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 K	5 B 0 1 7
3/06	3 0 1	3/06	3 0 1 A	5 B 0 6 5
12/00	5 3 7	12/00	5 3 7 A	5 B 0 8 2

審査請求 未請求 請求項の数 9 O L (全 17 頁)

(21) 出願番号 特願2001-213642 (P2001-213642)

(22) 出願日 平成13年7月13日 (2001.7.13)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 伊東 隆介

神奈川県小田原市中里322番地2号 株式

会社日立製作所 R A I D システム事業部内

(72) 発明者 岡見 吉規

神奈川県小田原市中里322番地2号 株式

会社日立製作所 R A I D システム事業部内

(74) 代理人 100075096

弁理士 作田 康夫

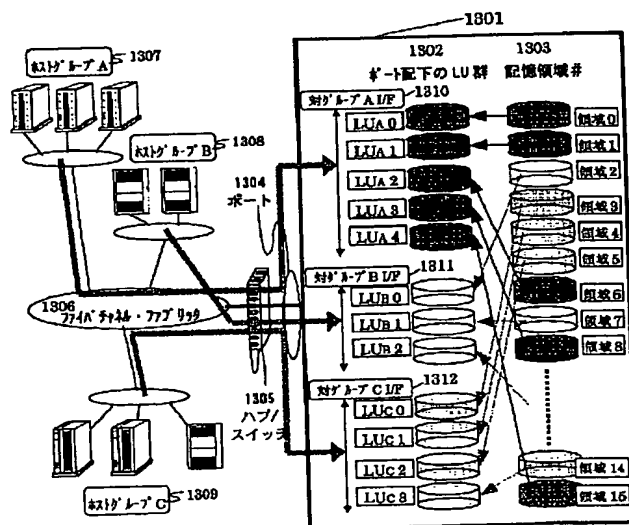
最終頁に続く

(54) 【発明の名称】 論理ユニット毎のセキュリティ機能を備えた記憶サブシステム

(57) 【要約】 (修正有)

【課題】 多種多様なコンピュータからのアクセスが想定される記憶サブシステムにおいて、従来の L U N セキュリティ機能ではシステムの資源の有効利用を図りつつ、論理ユニット単位でのセキュリティを実現できなかった。

【解決手段】 コンピュータを一意に識別する情報 W W N (World Wide Name) と、このコンピュータが属するグループを識別する情報 G I D (Group ID) と、このホストコンピュータからのアクセスを許可した記憶サブシステム内の論理ユニット番号 L U N を、ユーザ任意の運用方法に基づいて規定し、ホストコンピュータに対して開示するテーブルを設ける。記憶サブシステム内の管理テーブルを用いることによって、ユーザが任意にグループ化したコンピュータ群に対し、そのグループ単位で記憶サブシステム内の論理ユニットに対するアクセス可否を決定できる。



## 【特許請求の範囲】

【請求項 1】複数のコンピュータに接続するためのインタフェースを適用可能なポートと、前記ポートを経由して前記コンピュータからアクセス可能な論理ユニットと、前記論理ユニットに格納すべきデータを格納する 1 つ又は複数の記憶装置と、

前記記憶装置に対してデータの読み書きを制御する記憶制御装置を有する記憶サブシステムにおいて、前記論理ユニットにアクセスするコンピュータを、重複を許して、グループに分け、各グループに 1 つ又は複数の論理ユニットを割り当て、割り当てた論理ユニットと前記記憶装置の記憶領域とを、重複を許して、対応させる管理テーブルを設けたことを特徴とする記憶サブシステム。

【請求項 2】請求項 1 記載の記憶サブシステムであって、前記管理テーブルは、更に、前記グループ分けしたコンピュータの各グループと、前記割り当てられた論理ユニットとを対応させるインタフェース情報を有する記憶サブシステム。

【請求項 3】請求項 1 記載の記憶サブシステムであって、更に、保守用端末装置を接続可能な通信制御部を有し、前記通信制御部に通信回線を介して保守用端末装置を接続し、前記管理テーブルの内容を変更できる記憶サブシステム。

【請求項 4】請求項 1 記載の記憶サブシステムにおいて、前記割り当てた論理ユニットと前記記憶装置の記憶領域とを、重複を許して、対応させることにより、前記グループ分けされた各グループ相互の論理ユニット単位でのセキュリティを機能させることを特徴とする記憶サブシステム。

【請求項 5】請求項 1 記載の記憶サブシステムにおいて、前記ポートを経由してアクセスしてくるコマンドから、そのコマンドを送出したコンピュータを特定する情報を抜き出し、その特定する情報が前記管理テーブルに存在したときは、前記グループに分けたコンピュータであるとして、前記割り当てた論理ユニットへのアクセスを許し、その特定する情報が前記管理テーブルに存在しなかったときは、前記グループに分けたコンピュータでないとして、前記アクセス可能な論理ユニットへのアクセスを許さない機能を有する記憶サブシステム。

【請求項 6】請求項 5 記載の記憶サブシステムにおいて、前記機能を、コンピュータの問合せコマンド発行の際にのみ発揮させ、一度、前記割り当てた論理ユニットへのアクセスを許した後は、前記問合せに係るコンピュータ

からのコマンドを受け付ける記憶サブシステム。

【請求項 7】請求項 6 記載の記憶サブシステムにおいて、前記割り当てた論理ユニットへのアクセスを許した後は、当該論理ユニットの番号と、当該論理ユニットに対応した前記記憶装置の記憶領域の番号との対応付けには、前記問合せに係るコンピュータのグループの番号を使用する記憶サブシステム。

【請求項 8】複数のコンピュータ又は記憶サブシステムに接続するためのインタフェースを適用可能なポートと、前記ポートを経由して前記コンピュータからアクセス可能な論理ユニットと、前記論理ユニットに格納すべきデータを格納する 1 つ又は複数の記憶装置と、前記記憶装置に対してデータの読み書きを制御する記憶制御装置を有する記憶サブシステムにおいて、前記論理ユニットにアクセスするコンピュータを、重複を許して、グループに分け、各グループに 1 つ又は複数の論理ユニットを割り当て、割り当てた論理ユニットと前記記憶装置の記憶領域とを、重複を許して、対応させる管理テーブルを、前記ポートを介して接続された記憶サブシステムと共用することを特徴とする記憶サブシステム。

【請求項 9】複数のコンピュータ、ハブ、スイッチ又はルーターに接続するためのインタフェースを適用可能なポートと、前記ポートを経由して前記コンピュータからアクセス可能な論理ユニットと、前記論理ユニットに格納すべきデータを格納する 1 つ又は複数の記憶装置と、前記記憶装置に対してデータの読み書きを制御する記憶制御装置を有する記憶サブシステムにおいて、前記論理ユニットにアクセスするコンピュータを、重複を許して、グループに分け、各グループに 1 つ又は複数の論理ユニットを割り当て、割り当てた論理ユニットと前記記憶装置の記憶領域とを、重複を許して、対応させる管理テーブルを、前記ポートを介して接続されたコンピュータ、ハブ、スイッチ又はルーターと共用することを特徴とする記憶サブシステム。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】コンピュータからアクセスされる記憶サブシステムに係り、特に、記憶サブシステム内の論理ユニットのアクセスに関する。

【0002】

【従来の技術】近年、ファイバチャネル・プロトコルが規格化され、それをインフラとして SAN (Storage Area Network) 環境が複雑、多様化し

てきた。この結果、記憶サブシステムにつながるコンピュータの数と種類若しくはOS (Operation System) の種類、並びに記憶サブシステムに要求される論理ユニット数が大幅に増加している。また記憶サブシステムとコンピュータとのインタフェースに、ファイバチャネルの他、SCSIや、ESCON、TCP/IP、iSCSIなど様々なプロトコルが同時に使用される環境が整いつつある。尚、ここで、コンピュータとは、ネットワークに接続可能な電子回路を有する電子機器をいう。

【0003】このような環境では、多種多様のコンピュータが1つの記憶サブシステムに対してアクセスしてくることを意味する。コンピュータには、いわゆる大型のホストコンピュータや、小型の個人用のコンピュータも含まれるが、種々のコンピュータが記憶サブシステムにアクセスする場合に、適宜、「ホストからアクセスする」、「ホストコンピュータからアクセスする」等の表現を用いる。

【0004】この状況下では従来のホスト側のOSやミドルウェア、アプリケーション・ソフトウェアに頼った記憶サブシステム資源に対するセキュリティ機能では不十分であると危惧されるようになり、論理ユニット（以下、適宜、LUと略す）に対する不正アクセスを防止する強固なLUNセキュリティ機能の必要性も急速に高まってきている。尚、LUNとは、記憶サブシステム内の論理ユニット番号をいう。

【0005】記憶サブシステム資源（論理ユニット）に対するセキュリティ機能の実現手段として、特開2000-276406がある。左記公報による方法では、記憶サブシステム内のLUNに対するアクセス可否に関して、セキュリティ機能を実現しているものの、単一のポートに対してアクセスしてくる多種多様のコンピュータには、対応できず、実際の運用上は単一ポート配下で管理可能なホストコンピュータ種を1種類とするものである。この実際の運用上の制限は、先に述べたSAN環境の急激な拡張等の状況に追従できない。

【0006】

【発明が解決しようとする課題】記憶サブシステム内の論理ユニットを、LUNセキュリティ機能を伴いつつコンピュータに提供すべく、記憶サブシステムの単一ポート配下に、従来よりも多数の論理ユニットを定義づけ、複数のOSを有するホストコンピュータ、OSの種類が異なる複数のコンピュータその他コンピュータ群に開示する必要がある。

【0007】しかし従来の記憶サブシステムのLUNセキュリティ機能では、単一ポート配下で管理可能なホストコンピュータが多数あってもOSの種類は同一でなければならず、さらに単一ポートに設定可能なホストコンピュータとの接続上のインターフェース設定も1通りのみという制限が一般的であり、最近のSAN環境に対す

る課題となっていた。このような課題を解決すべく、単純に、記憶サブシステムの単一ポート配下に多数の論理ユニットを定義し、当該ポートにアクセスしてくる複数種類のOSに対して、そのまま分割・開示する方法が考えられる。

【0008】しかし、現状のコンピュータの種々のOSは、記憶サブシステムの論理ユニットゼロ(LU0)にアクセスできない場合には、そのLU0の次のLU1以降の同系列のLUに対しては、その存在を全く問いつけない仕様となっている。因みに、SCSI-2の規格では、この1系列は8つのLUで構成されるため、LU0~LU7までが同系列となる。

【0009】このため、記憶サブシステム内の論理ユニット番号(LUN)をそのままホストコンピュータに開示したのでは、論理ユニット設定側の期待通りには、コンピュータに論理ユニットが正しく認識されないという課題があった。

【0010】また、現状のコンピュータの種々のOSは、単一ポート配下に認識し得る論理ユニット数の上限を256個とするものが多く、論理ユニット数を257個以上設けても認識されないこととなり、この点も記憶サブシステム内の論理ユニットを単一ポート配下でコンピュータに開示する上での課題となっていた。

【0011】一方、記憶サブシステムにおいて、強固なLUNセキュリティ機能を提供する場合において、コンピュータから送信されてくるコマンドに関して、逐一、対象LUに関するアクセス可否をチェックする方法が最も堅牢ではあろうが、記憶サブシステムにおける処理時間（セキュリティチェックのためのオーバーヘッド）が大きくなってしまい性能上の課題となっていた。

【0012】そこで、本発明の第1の目的は、コンピュータの既存の処理、制限その他の機能を変更せずに、コンピュータをOSその他任意の種別毎にグループ化して、そのグループ化されたコンピュータがアクセス可能な論理ユニットを制限し、そのグループ単位にインターフェース上の設定を可能とし、LUNセキュリティ機能を記憶サブシステムの単一ポート配下において提供可能とすることである。また、本発明の第2の目的は、上記セキュリティ機能を、記憶サブシステムの高速なアクセス判定ロジックと共に提供することである。

【0013】

【課題を解決するための手段】記憶サブシステムを次の構成とする。即ち、コンピュータ（ホストコンピュータを含む）を一意に識別する情報（WWN:World Wide Name）、このコンピュータが属するグループを識別する情報（GID:Group ID）、このコンピュータからのアクセスを許可した記憶サブシステム内の論理ユニット番号（LUN）の対応を記述した管理テーブルと、これを格納する不揮発のメモリと、コンピュータが記憶サブシステムにログインする際に動的に割

り当てられ、以降、ログアウトするまで有効であるユニークな管理番号(S\_ID)、コンピュータを一意に識別する情報(WWN)、およびこのホストコンピュータが属するグループを識別する情報(GID)の対応を記述した管理テーブルと、これを格納する不揮発のメモリと、これら管理テーブルを設定する1つ以上の入力端末と、1つ以上の記憶装置と、これらの記憶装置に対してデータの読み書きを制御する記憶制御装置と、コンピュータと接続を行うための1つ以上のポートと、前記記憶装置の記憶領域に対応した論理ユニット(LUN)を有する記憶サブシステムとする。

【0014】この記憶サブシステムにおいては、コンピュータの既存の処理、制限その他の機能を変更せずに、単一ポート配下で、ユーザが、任意のコンピュータのグループ単位に、アクセス可能なLUN設定や接続インターフェース上の設定を行なえるため、単一ポート配下で、複数の種類のOSを備えたコンピュータ群を対象に、アクセスコントロール機能、すなわちLUNセキュリティ機能を実現することができる。

【0015】また、この記憶サブシステムにおいては、ホスト識別情報WWNの代わりに、ログインの際に割り当てるS\_IDをもとにGIDを識別情報として用いるため、アクセス可能なLUNを判定する際の時間が、WWNを用いる場合に比べて簡易であるため少なくて済み、高速である。

【0016】

【発明の実施の形態】本発明では、記憶サブシステムとコンピュータ間で使用するインタフェース・プロトコルの例としてファイバチャネルを用い、その上で動作するコマンドセットの例としてSCSIコマンドを用いて説明する。尚、本発明は、ファイバチャネルとSCSIコマンドの組み合わせに限定されるものではなく、これらと同様に、ログイン、問い合わせ、ログアウトといった機能・機構を提供可能なプロトコルであればどのような組合せ、インタフェースであっても適用可能である。

【0017】本発明の第一の実施例を以下に示す。初めに、ファイバチャネルのプロトコル上で本発明に係る特徴を説明する。ファイバチャネルのインタフェースを持つ機器をノードと呼び、実際のインタフェースにあたる物理的な端子をポートと呼ぶ。ノードは1つ以上のポートを持つことが可能である。ファイバチャネルの系全体に同時に参加できるポートの数は、最大で24ビットのアドレス数、すなわち、2の24乗個(16777216個)である。これらの接続を媒介するハードウェアをファブリックと呼ぶ。実際には、送信元および送信先のポートは、ファブリックを意識せずに互いのポートに関する情報のみを考慮して動作すればよい。

【0018】各ノードおよびポートには、標準化団体(IEEE)から一定のルールによって割り当てられる、世界中でユニークな識別子が記憶されている。これ

は従来からTCP/IPなどで馴染みのMACアドレスに相当するものであり、ハードウェア的に固定なアドレスである。このアドレスにはN\_Port\_Name、Node\_Nameの2種類があり、それぞれ8バイトのサイズを持つ。N\_Port\_Nameはポート毎に固有の値(ハードウェア・アドレス)であり、Node\_Nameはノード毎に固有の値(ハードウェア・アドレス)である。これらは、いずれも世界中でユニークな値であることから、ノードまたは、ポートを一意に識別できるアドレスとして、WWN(World Wide Name)と呼ばれる。本特許の実施例では、WWNと記述した場合、N\_Port\_Nameを指すものとする。

【0019】ファイバチャネルでは、通信はOrdered Setと呼ばれる信号レベルの情報と、フレームと呼ばれる固定のフォーマットを持った論理的な情報とで行われる。図2はフレームの構造を示している。フレーム201は、フレームの始まりを示すSOF(Start of Frame)202と呼ばれる4バイトの識別子、リンク動作の制御やフレームの特徴づけを行う24バイトのフレームヘッダ203、実際に転送される目的となるデータ部分であるデータフィールド204、4バイトの巡回冗長コード(CRC)205、フレームの終わりを示すEOF(End of Frame)206と呼ばれる4バイトの識別子からなる。データフィールド204は0~2112バイトの間で可変である。

【0020】次に、フレームヘッダの内容について説明する。207はフレームヘッダの構造について示している。ここではフレームヘッダ203の詳細構造207における、1ワード目の0~23ビット領域にあたるS\_ID208についてのみ説明する。S\_ID(Source ID)208は当該フレームを送信するポートを識別するための3バイトのアドレス識別子であり、送受信されるすべてのフレームで有効な値を持つ。このS\_IDは動的に変動する値であり、ファイバチャネルの規格セットの1つであるFC\_PHでは、S\_IDをファブリックによって、初期化手続き時に割り当てられる、としている。割り当てられる値は、それぞれのポートがもつN\_Port\_Nameまたは、Node\_Nameに依存する。

【0021】次に、ファイバチャネルプロトコルに基づく、送信元の機器と送信先の機器が通信に関して互いに情報を交換するログイン手続きについて述べる。図3は、送信元(ログイン要求元)301と送信先(ログイン受信先)302との間に取り交わされる情報のやりとりを示したものである。

【0022】ファイバチャネルのログイン手続きには数種類存在するが、ここではクラス3のログインに関して述べる。ログイン要求元は、PLOGIフレーム303をログイン受信先へ送信する。このフレームには、ログ

イン要求元のN\_Port\_Name、Node\_Name、S\_IDおよびその他の情報が含まれている。

【0023】受信先の装置では、このフレームに含まれている情報を取り出し、ログインを承認する場合は、ACC304と呼ばれるフレームをログイン要求元に対して送信する。一方、ログインを拒絶する場合は、LS\_RJT305と呼ばれるフレームをログイン要求元に対して送信する。

【0024】ログイン要求元は、自らが送信したPLOGIフレームに対してACCフレームの応答を検出すると、ログインが成功したことを知り、データ転送などのI/Oプロセスを開始できる状態となる。一方、ログイン要求元が、LS\_RJTを受信した場合はログインが成立しなかったこととなり、当該ログイン受信先へのI/Oプロセスは実行不可となる。

【0025】ここではクラス3のログインについて述べたが、他のログインプロセスにおいても、ログイン要求元からログイン受信先へ渡すことのできる情報の中に、N\_Port\_Name、Node\_NameおよびS\_IDが含まれることにおいては同様である。

【0026】次に、SCSIコマンドセットでは必ずサポートされている標準的なコマンドである、Inquiryコマンドについて説明する。Inquiryコマンドとは、I/Oプロセスを開始するのに先立ち、I/Oプロセスの対象となる論理ユニットに対して、その実装状態、準備状態を問い合わせるコマンドである。図4は、SCSI規格で定義されたInquiryコマンドを、ファイバチャネル規格のフレームで送信する場合のデータフィールドの詳細構造を示している。フレーム、およびフレームヘッダの基本構造は図2と同様である。よって、S\_ID405が含まれている。

【0027】データフィールド403には406のFCP\_CMNDフォーマットに示すように、FCP\_LUN407、FCP\_CNTL408、FCP\_CDB409、FCP\_DL410と呼ばれる領域がある。ここではFCP\_LUN407、およびFCP\_CDB409について述べる。

【0028】FCP\_LUN407の中には、フレーム送信元が状態を問い合わせようとする、フレーム送信先のポートに関連付けられた論理ボリュームの識別子が格納されている。尚、論理ボリュームとは、目に見える単体としての記憶装置（物理ボリューム）に対して、便宜上仮想的に分割されナンバリングされた記憶領域をいう。また、この識別子をLUN(Logical Unit Number)という。

【0029】FCP\_CDB409の中には、SCSIコマンドセットを使用する場合にはSCSIのコマンド記述ブロック(CDB)と呼ばれる命令情報が格納される。このFCP\_CDB409の中に、SCSIのInquiryコマンド情報が格納されて、前述のFCP\_

LUN 407と共に、フレーム受信先へ情報が転送される。

【0030】SCSIコマンドセットでサポートされているその他のコマンド、例えば、WriteコマンドやReadコマンド等でも、フレームはInquiryコマンドと同様、401や406の構造である。したがって、本発明の実施に必須であるS\_IDやFCP\_LUNを含むことは、それらのコマンドにおいても共通である。

【0031】図5に、このInquiryコマンドを用いた論理ユニット問合せの手順を示す。論理ユニットにアクセスしようとするホストコンピュータ501は、アクセスしようとする論理ユニットをもつ記憶サブシステム502に対し、Inquiryコマンドを格納したフレーム503を送信する。このフレームには、ホストコンピュータのS\_IDと、問合せを行う先の論理ユニットの識別子であるLUNが含まれている。ここで、LUNについては、FCP\_LUN領域の他に、FCP\_CDB内のInquiryコマンド情報のフォーマット中にも設定することができる。どちらの値を使用しても得られる効果は同じであるが、本実施例ではLUNの値はFCP\_LUN407に格納された値を使用するものとする。

【0032】Inquiryコマンドを含むフレームを受信した記憶サブシステム502は、問合せに対して必要なInquiryデータを準備し、作成したInquiryデータを含むフレーム504をホストコンピュータに送信する。このときInquiryデータを格納するフレームを、FCP\_DATAと呼ぶ。記憶サブシステムが、問合せのあった論理ユニットについて、クオリファイア000(2進数)、デバイスタイプ00~09(16進数)のいずれかを設定する場合(504)、このInquiryデータを受信したホストコンピュータは、当該論理ユニットに対して、以降I/Oの発行が可能となる。

【0033】一方、505に示すように、記憶サブシステムが、クオリファイア001(2進数)または011(2進数)、デバイスタイプ1F(16進数)を設定した場合、このInquiryデータ505を受信したホストコンピュータは、当該論理ユニットに対して、以降、I/Oの発行が不可能であることを認識する。以上のことから、Inquiryデータに格納するクオリファイア、およびデバイス・タイプ・コードを、記憶サブシステム側でコントロールすれば、ホストコンピュータから記憶サブシステムの論理ユニットへのアクセス許可および不許可を制御できることが分かる。

【0034】先に述べたように、Inquiryコマンドの以外のWriteコマンドやReadコマンド等でも、基本的なフレームの作りは401のように共通である。したがって、送信先の記憶サブシステムが、送信元

のホストコンピュータが指定したS\_IDやLUNが不正と検出すれば、アクセス拒否をすることが可能である。

【0035】続いて、本発明の処理の流れについて詳細を述べる。図1は、本発明の実施例の装置構成を示したものである。記憶サブシステム101は、ファイバチャネル・インタフェース用のポート102~104を有し、ファイバチャネル・インタフェースを介して、ホストコンピュータ105~107と物理的に接続されている。ホストコンピュータ105~107もまた、ファイバチャネルインタフェース用のポート108~112を有しており、ホストコンピュータ105~107と記憶サブシステム101は、ファイバチャネル・プロトコルによる通信が可能となっている。ホストコンピュータには、105や106のように複数のファイバチャネル・ポートをもつものもあれば、107のように単一のファイバチャネル・ポートしかもないものもある。記憶サブシステム101とホストコンピュータ105~107間のファイバチャネルインタフェースの接続形態（トポロジ）には、Point-to-Pointや、アービトラレーション・ループ接続、ファブリック接続等、いくつかの種類が存在するが、本発明はその接続形態には依存しないため、単にファイバチャネル113と記述する。

【0036】まず、記憶サブシステム101は、種々の演算や処理を行うマイクロプロセッサ114を有し、複数の記憶装置群115、およびこれらにデータの読み書きを制御して行う記憶制御装置116、さらに記憶装置群115と記憶制御装置116を接続するためのバス117を有している。

【0037】また、記憶サブシステム101は、種々の演算や処理のワーク領域として使用するメモリ118と、種々の管理情報、管理テーブル等を保存しておく不揮発メモリ119を有する。更に、ホストコンピュータへの応答を速くするための工夫として、キャッシュ120を有している。

【0038】また、記憶サブシステム101は、通信制御部121を有し、通信回線122を介して、保守用端末装置123と接続されている。

【0039】保守用端末装置123は、内部にマイクロプロセッサ124と、ユーザとのインタフェースとなる入力部125と処理の結果を出力する表示部126を有している。ユーザは、この入力部125を介して、本実施例で定義するいくつかのテーブルの設定を行うことができる。

【0040】マイクロプロセッサ114、メモリ118、不揮発メモリ119、通信制御部121は図1のように、別個の構成としても良いし、記憶制御装置116の内部に配置しても良い。キャッシュ120の物理的形状（大きさ）により記憶制御装置116の内部に設けることができないときは、外部に所定のバス（経路）によ

って接続する。この場合には、ポート102~104の直下に記憶制御装置116が配置され、所定のバスにより各ポートと記憶制御装置116とが接続される構成となる。また、記憶制御装置116がマイクロプロセッサ114で為される機能を代替することも可能である。通信制御部121に接続される保守用端末装置123は、記憶サブシステム101の内部に設置しておくこと（常時接続）も、また、必要なときのみ通信回線122を介して接続すること（保守時接続）も可能である。

【0041】図6において、本実施例の処理流れ概要を示す。手順601において、ユーザは前述の保守用端末装置123の入力部125を介して、記憶サブシステム内に存在する論理ユニット（LU）を規定するLUN

（Logical Unit Number）と、そのLUNにアクセスする可能性のあるホストコンピュータのWWN（N\_Port\_Name）と、これらアクセスする可能性のあるホストコンピュータをユーザが任意にグループ化した際に割り当てるGID（Group ID）を結びつけた「LUNアクセス管理テーブル」を作成する。本テーブルは、記憶サブシステム内の不揮発メモリ119に保持される。各ホストコンピュータには、本テーブルのLUNが見える。各ホストコンピュータのWWNは既知である。

【0042】手順602において、各ホストコンピュータが記憶サブシステムに対して、ファイバチャネル・プロトコルに基づいてログインしてくると、記憶サブシステムはPLOGIフレームから、当該ホストコンピュータのWWNと、S\_IDを切り出し、同時に手順601でユーザが作成した「LUNアクセス管理テーブル」から当該のWWNが属するGIDを検索し、それらの組み合わせを記述した「WWN\_S\_ID\_GID変換テーブル」を作成し、不揮発メモリ119上にこれを保持する。

【0043】「LUNアクセス管理テーブル」から、当該WWNが属するGIDが検索されない場合は、ユーザが当該WWNの属するホストコンピュータ・グループを定義しなかったことを意味する。したがって、この場合は「WWN\_S\_ID\_GID変換テーブル」の当該WWNに対応するGIDには未定義のIDが登録される。記憶サブシステムはこの作業を全てのPLOGIフレームに対して行う。

【0044】手順603において、記憶サブシステムは、各ホストコンピュータが記憶サブシステム内の論理ユニットの状態を知るために送信したInquiryコマンドを含むフレームを受信する。このフレームを受信した記憶サブシステムは、そのフレームのヘッダからS\_IDを、データフィールドからInquiryコマンドの対象となるLUNを切り出す。続いて、記憶サブシステムは、このS\_IDをキーにして上述の「WWN\_S\_ID\_GID変換テーブル変換テーブル」を検索し、こ



のS\_IDに対応するG\_IDを取得する。

【0045】手順604において、記憶サブシステムは、得られたG\_IDをキーにして上述の「LUNアクセス管理テーブル」から、Inquiryコマンドの対象となっているLUNを検索する。手順605では、手順604の結果、当該G\_IDに対応するLUNを取得できたか否かの判定を行う。取得できた場合、すなわち当該G\_IDに対応するLUNが「LUNアクセス管理テーブル」上に存在した場合は、当該ホストコンピュータの属するホストコンピュータ・グループによる当該LUNへのアクセスが許可される。一方、LUNが該テーブルに存在しない場合は、当該ホストコンピュータの属するホストコンピュータ・グループによる当該LUNへのアクセスは拒絶される。

【0046】手順605の結果、当該ホストコンピュータによる当該LUNへのアクセスが許可される場合、記憶サブシステムは、手順606において、ホストコンピュータの発行したInquiryコマンドに対して、対象LUが実装済みの設定（すなわちアクセス可能である旨の設定）を行った上で、Inquiryデータを送信する。一方、当該LUへのアクセスが拒絶される場合、記憶サブシステムは、手順607によって、ホストコンピュータの発行したInquiryコマンドに対して、対象LUが未実装の設定、すなわちアクセス不可である旨の設定を行った上で、Inquiryデータを送信する。

【0047】Inquiryデータを受信したホストコンピュータは、そのフレームを解析し、解析の結果、記憶サブシステムの当該仮想LUNへのアクセスが許可されたことを認識すると、ホストコンピュータは以降、当該LUNに対して、コマンド（I/O要求）を継続して発行することができる。この場合、手順608にあるように、記憶サブシステムは当該ホストコンピュータからのログインが有効である間は、当該LUへのコマンド受信を継続することができる。

【0048】一方、当該LUNへのアクセスが拒否されたことを認識したホストコンピュータは、記憶サブシステムへのログインが有効である間、当該LUへ再度アクセスすることはない。以下、上記の記憶サブシステム内の特定LUNに対するホストコンピュータからのアクセス可否を制御する方法を、「本発明におけるLUNセキュリティ」と呼ぶ。

【0049】次に、図7から図10を用いてもう少し詳細に技術的課題を説明し、図11から本発明について説明する。はじめに、上記手順601の「LUNアクセス管理テーブル」の作成について記述する。本発明におけるLUNセキュリティは、記憶サブシステムのもつポート毎に管理され、ホストコンピュータは、この記憶サブシステムのポートを通して、記憶サブシステム内のLUにアクセスするものとする。この場合、最も簡単な方法

として、ホストコンピュータを一意に識別する情報であるWWNと、当該ホストコンピュータにアクセスを許可するLUNの対応を定義した、図7に示すようなテーブル701を、記憶サブシステム内に設ければよい。このことは、ホストコンピュータと記憶サブシステムとが専用の回線で接続されている場合には何ら問題なく、その機能を達成することとなる。

【0050】テーブル701は、記憶サブシステム内の記憶領域に対して、単一ポート配下で一意にナンバリングし、その論理ユニット番号（LUN）を、そのままホストコンピュータのWWNに対して割り当てている。図7では、WWN702のホストコンピュータには、LU0～2にのみアクセスが許可され、WWN703のホストコンピュータは、LU3、4、および7にのみアクセスが許可され、WWN704のホストコンピュータは、LU5～6にのみアクセスが許可されている。

【0051】したがって、例えばLU0～2は、WWN702のホストコンピュータ以外のホストコンピュータからは、アクセス不可となり、本発明におけるLUNセキュリティが実現されるからである。

【0052】しかし、ホストコンピュータと記憶サブシステム間に、ファイバチャネル対応のハブや、スイッチなどの機器類が介在するような最近の複雑な使用環境下では、701のテーブルだけでは不十分である。今日、多くのホストコンピュータでは、接続されている記憶サブシステムのLU0にアクセスできない場合には、そのLU0以降の同系列のLU（SCSI-2の規格では、この1系列は8つのLUで構成されるため、LU0～LU7までが同系列となる。）には全く存在の問い合わせをしない、とするものが多いためである。このようなホストコンピュータからアクセスがあった場合、テーブル701のような規定方法では、ホストコンピュータ703や704は、アクセスを許可するLUNがそれぞれ規定されていながら、LU0にアクセスできないために、テーブル701で規定したアクセス許可のLUNを参照できない事態が発生してしまう。併せて、このような現象は、ディスクアレイ装置のような記憶資源を豊富に提供し得る装置においては、著しくその利用率を下げ、記憶資源の無駄を生ずる。

【0053】そこで、これを防ぐためにホストコンピュータ703、704にLU0へのアクセスを許可すると、LU0の排他がなくなりセキュリティが保証されない。仮にこれを認めた場合にも、ホストコンピュータ703と704が異なるOSをもつホストコンピュータである場合、LU0を共有することは、それぞれのOSによるフォーマットの違いから困難でとなってしまう。

【0054】一方、図7において、記憶サブシステムの当該ポート配下にLU0の定義がなくても、全てのLUNに対して存在の問い合わせを行うことが可能な、WWN705～707を持つホストコンピュータ群が存在す

ると仮定する。ここでは、WWN705のホストコンピュータは、LU0、1、7にのみアクセスが許可され、WWN706のホストコンピュータは、LU3、5、6にのみアクセスが許可され、WWN707のホストコンピュータは、LU2、4にのみアクセスが許可されている。

【0055】この状態を視覚的に表したのが図8である。ホストコンピュータ802～804は、図7 WWN705～707を持つホストコンピュータに相当する。ホストコンピュータ802～804は、ファイバチャネル対応のハブ、スイッチ又はルーター805を経由して記憶サブシステムの同一のポート806に接続している。このような使用環境において、各々のホストコンピュータ802～804に対し、無計画にアクセス対象LUNを定義したり、以前割り当てたLUNと異なるLUNをアクセス対象として割り当てた場合、記憶サブシステム内の同一ポート配下で一意にナンバリングしたLUNをそのままホストコンピュータに開示している801のような記憶サブシステムではLUNの開示方法に柔軟性がなく、当該ポート配下が、LU群807のようにLUが離散した状態で見え、使用上、著しく管理しにくい状態となってしまう。

【0056】一方、最近、記憶サブシステムの1つのポート配下に9個以上のLUを定義しても、これを認識するホストコンピュータが存在するが、このようなホストコンピュータと従来のように1つの記憶サブシステムのポート配下にLU0～7までの8個のLUしかサポートしないホストコンピュータ間でLUNセキュリティを実施した場合の問題点を示す。

【0057】図9において、WWN902、904を持つホストコンピュータが、接続する記憶サブシステムのポート配下にLU0が存在しなくても、各LUに存在の問い合わせを行う機構をもち、かつ、接続する記憶サブシステムのポート配下にLUを16個まで認識する場合について以下説明する。

【0058】WWN903を持つホストコンピュータは、接続する記憶サブシステムのポート配下にLU0が存在しなくても、各LUに存在の問い合わせを行えるが、サポート可能なLUはLU0～7の範囲の8個までとする。テーブル901から分かるように、WWN902を持つホストコンピュータはLU0～5の範囲でアクセスが許可されており、WWN903を持つホストコンピュータはLU6～10の範囲で、またWWN904を持つホストコンピュータはLU11～15の範囲でアクセスが許されている。この状態を視覚的に表したのが図10である。

【0059】ホストコンピュータ1002～1004は、図9のWWN902～904を持つホストコンピュータに相当する。ホストコンピュータ1002～1004は、ファイバチャネル対応のハブ、スイッチ又はルー

ター1005を経由して記憶サブシステムの同一のポート1006に接続している。このような使用環境において、各々のホストコンピュータ1002～1004に対して、LU群1008のように記憶サブシステム内のLUを割り当てたとすると、ホストコンピュータA1002には、LU群1008中のLU0～5の範囲のみアクセス許可対象として見え、ホストコンピュータC1004には、LU群1008中のLU11～15の範囲のみアクセス許可対象として見え、それぞれLUNセキュリティの目的を果たすことができる。しかし、ホストコンピュータB1003は、元々1ポート配下にLU0～7までの範囲で、8個までしかLUを認識できないため、LU群1007の範囲内でしか問い合わせを実施することができない。よって、テーブル901において、LU6～10までアクセス許可をしても、実際には、LU6、7にしかアクセスできないという問題が生じる。これも、記憶サブシステム内の同一ポート配下で一意にナンバリングしたLUをそのまま開示しているために起こる弊害である。

【0060】以上のような懸念を考慮して、本発明では、図11に示すような「LUNアクセス管理テーブル」1101を定義する。テーブル1101は、図7のテーブル701、図9のテーブル901のように記憶サブシステム内の同一ポート配下で一意にナンバリングしたLUNを単にWWNに直接割り当てたテーブルとは異なる。

【0061】テーブル1101は、アクセスする可能性のあるホストコンピュータのWWNと、これらホストコンピュータ群をユーザが任意にグループ化した際に割り当てるGID(Group ID)を結びつけ、これらホストコンピュータ・グループに対して、記憶サブシステム内のアクセスを許可できる記憶領域に、ユーザが任意に設定できる論理ユニット番号(LUN)を付与するものである。

【0062】本テーブルは、記憶サブシステムのポート単位に作成される。この「LUNアクセス管理テーブル」1101を定義した記憶サブシステムでは、ユーザが任意にグループ化したホストコンピュータ群に対して、ユーザの使用希望に沿った形でLUNを柔軟にナンバリングし、それらを開示することができる。

【0063】通常、OSが異なると、LUに対する論理フォーマットが異なるため、異OS間でのLUの共有はできない。したがって、「LUNアクセス管理テーブル」1101において、ユーザが登録するグループは、通常、同一のOSを搭載したホストコンピュータ群となる。

【0064】このホストコンピュータ・グループ登録において、ユーザの使用希望条件(例えば、交替パス構成、ホストコンピュータ間のクラスタ構成等)をより詳細に組み込めば、更にユーザの使い勝手を向上させるこ

とができ、同時に記憶サブシステム内の記憶領域を有効利用することができる。「LUNアクセス管理テーブル」1101の詳細な設定例を図11を用いて説明する。1101において、WWN1112~WWN1114をもつホストコンピュータ群は、同一のOS種1を搭載し、GroupA 1105としてカテゴリ化されている。これらのホストコンピュータ・グループには記憶サブシステム内のLU0~3へのアクセスが許可されている。記憶サブシステム内では、これらLU0~3には記憶領域番号0~3（以下、適宜、記憶領域#0~3と略記する）が割り当てられている。

【0065】また、WWN1115~WWN1117をもつホストコンピュータ群は、同一のOS種2を搭載し、GroupB 1106にカテゴリ化されている。これらホストコンピュータ・グループには、やはりLU0~3がアクセス許可されているように見えるが、記憶サブシステムの内部ではこれらLU0~3には、記憶領域#60~63が割り当てられており、上述のGroupA 1105の使用記憶領域とは排他がなされており、本発明におけるLUNセキュリティが実現されている。

【0066】一方、WWN1118~WWN1121をもつホストコンピュータ群は、GroupC 1107にカテゴリ化されているが、その内訳は、OS種3を搭載したホストコンピュータ群とOS種4を搭載したホストコンピュータ群の混在である。通常、OS種が異なると論理フォーマットが異なるため、LUの共有ができないが、共有可能な異なるOS種が存在する場合、このようなグループ化も可能である。、GroupC 1107には、LU0~5が連続してアクセス許可されているように見えるが、実際には離散した記憶領域#7、11、70、79、87、119が割り当てられている。

【0067】また、WWN1122、1123をもつホストコンピュータ群は、GroupD 1108にカテゴリ化されているが、それぞれOS種5、OS種6という異なるOS種を搭載している。GroupD 1108のホストコンピュータ群は、アクセスするポート配下にLU0が存在しなくても、その他のLUを離散的に認識する先進的なアーキテクチャをもっているため、LU50、LU51、LU62という複雑な開示方法でアクセス可能なLUが定義されている。これらアクセス可能なLUには、それぞれ記憶領域#40、99、100が割り当てられている。

【0068】「LUNアクセス管理テーブル」1101へのグループ登録は、必ずしも複数ホストコンピュータから成る必要はない。例えば、WWN1124のホストコンピュータに対して、単独でアクセス許可するLUを規定したい場合、ホストコンピュータ1台からなるGroupE 1109を登録すればよい。このような登録方法により、アクセス許可するホストコンピュータの分

解能を上げることができる。GroupE 1109には、LU0~1へのアクセスが許可され、そこには記憶領域#4、5が割り当てられている。

【0069】また、最近のSAN環境において問題となっている制限に対する解決策を示す。WWN1125および、1126のホストコンピュータは、共に単一ポート配下に256個のLUまでしか認識できないOS種7として、GroupF 1110にカテゴリ化されている。しかし、実際には単一ポート配下で512個のLUを認識させたいというユーザ要求があると仮定する。この場合、WWN1125および、1126のホストコンピュータを別グループGroupG 1111として再度登録する。両ホストコンピュータは、いずれも256個のLUまでしか認識しないため、GroupF 1110にはLU0~255まで、GroupG 1111にもLU0~255までをアクセス許可LUとして定義する。ただし、GroupF 1110のLU0~255には記憶領域#0~255を、GroupG 1111のLU0~255には記憶領域#256~512を割り当てることにより、ホストコンピュータの既存の処理、制限その他の機能を変更せずに、512個のLUを開示しながら、本発明におけるLUNセキュリティ機能を実現している。

【0070】最後に、上記とは異なる設定パターンを示す。WWN1129とWWN1130のホストコンピュータとWWN1131とWWN1132のホストコンピュータは、同一のOS種8を搭載した異なるフロアに存在するホストコンピュータである。これらのホストコンピュータを相手にする管理者は、これら4つのホストコンピュータに、異なるアクセスLUNでファイルやアプリケーションを開示したいが、開示する実体は同じ記憶領域の同じ内容としたい、と仮定する。そのような場合、テーブル1101のGroupH 1127とGroupI 1128のような設定を実施すればよい。この場合、GroupH 1127にはLU0、1が開示され、GroupI 1128には、LU4、5が開示されるが、実際の参照先記憶領域#は同一の10、11である。これら以外のホストコンピュータからのアクセスは拒絶される。これにより、上記管理者の目的にそった本発明におけるLUNセキュリティ機能を提供することができる。

【0071】以上、本発明の「LUNアクセス管理テーブル」によるホストコンピュータのグループ化とLUNの対応づけについて具体的に説明したが、これを視覚的に表すと図13のようになる。対応する「LUNアクセス管理テーブル」1201を図12に示した。

【0072】テーブル1201において、各ホストコンピュータ・グループ1205~1207にアクセスを許可したLU群1204は、実際には図13の記憶領域群1303のように全く乱雑な配置をとっている。しか

し、これをテーブル1201のLU群1204にマッピングすることで、図13のLU群1302の状態となり、ホストコンピュータグループ1307~1309に記憶サブシステム内の実際の記憶領域群の配置状態1303を意識させない状態でLUを開示することができる。尚、図13におけるホストコンピュータグループ1307~1309は、図12におけるホストコンピュータ・グループ1205~1207に相当している。

【0073】これにより、ホストコンピュータの既存の処理、制限その他の機能を変更せずに、本発明におけるLUNセキュリティが実現でき、記憶サブシステム資源の柔軟かつ効率的な運用も可能となる。

【0074】更に、このようなホストコンピュータのグループ化を実現することにより、記憶サブシステム1301内の単一ポート配下でありながら、ホストコンピュータ・グループ毎に記憶サブシステムとの接続インタフェース情報1310~1312（図13）を設定することができる。

【0075】接続上のインタフェース情報とは、例えば、記憶サブシステムの受領I/O、受領キューの深さであったり、Inquiryの応答内容等を指す。従来の記憶サブシステムでは、単一ポート配下のインタフェース情報は単一であるのが一般的であった。

【0076】本発明の「LUNアクセス管理テーブル」1101や1201は、図14の手順1401~1403に示すように、記憶サブシステムの全ポートに対して定義された後、記憶サブシステム内の不揮発メモリに保持される。不揮発メモリに保持されることで、本テーブルは、記憶サブシステムの電源切断によっても消失しない。また、所定の記憶装置115（記憶装置101、図1）に格納しても良い。

【0077】続いて、記憶サブシステムがホストコンピュータからログインされる際の処理について説明する。本実施例では、一連のログイン処理を通じて、ホストコンピュータを一意に識別するWWNからGID（グループID）取得し、ログイン以降に使用されるホストコンピュータを一意に識別するS\_IDとGIDを対応させる。

【0078】ホストコンピュータが起動すると、図15の手順1501において、記憶サブシステムは、PLOGIフレームを受信する。PLOGIフレームを受信した記憶サブシステムは、手順1502において、フレームヘッダからホストコンピュータのS\_IDを、手順1503において、データフィールドからホストコンピュータのWWN（N\_Port\_Name）を取得する。続いて、記憶サブシステムは手順1504において、このWWNとS\_IDとGID（グループID）を図16に示す「WWN\_S\_ID\_GID変換テーブル」1601に記録作成し、これを手順1505において、記憶サブシステム内の不揮発メモリに保持する。ここでGID

は、先に述べた、ユーザが設定する「LUNアクセス管理テーブル」からWWNをキーに検索することで得られる。「WWN\_S\_ID\_GID変換テーブル」1601は、記憶サブシステムのポート毎に作成される。

【0079】このテーブルに登録されたWWNをもつホストコンピュータから、以後、コマンドが送信されると、記憶サブシステムはそのフレームヘッダからS\_IDを取得し、「WWN\_S\_ID\_GID変換テーブル」1601を使用して、そのS\_IDに対応するGIDを知ることができる。記憶サブシステムは、この「WWN\_S\_ID\_GID変換テーブル」を不揮発メモリ上に保存すると、手順1506において、当該ホストコンピュータのログインを承認した旨のACCフレームを送信する。記憶サブシステムからACCフレームを受信したホストコンピュータは、これ以降、記憶サブシステムに対してInquiryコマンドを発行することができる。

【0080】続いて、ホストコンピュータからのInquiryコマンド受信と、これに対する記憶サブシステムのセキュリティ応答について説明する。図17、図18は、この一連の処理の流れを示したものであり、図19は、この一連の処理の流れにおいて使用される各テーブルやパラメータの参照関係を示したものである。

【0081】図17の手順1701において、記憶サブシステムは、ホストコンピュータからファイバチャネルに規定されたFCP\_CMNDフレームを受信する。すると記憶サブシステムは、手順1702において、そのFCP\_CMNDのデータフレームの内容を解析する。

【0082】続いて記憶サブシステムは、手順1703において、当該のFCP\_CMNDの内容がInquiryコマンドであるか否かをチェックする。Inquiryコマンドでない場合、記憶サブシステムは手順1704において、そのコマンドに対応した処理を実行する。一方、Inquiryコマンドであった場合、記憶サブシステムは手順1705において、当該FCP\_CMNDフレームのヘッダからホストコンピュータのS\_IDを取得し、手順1706において、当該FCP\_CMNDフレームのデータフィールドのFCP\_LUNから対象とするLUNを取得する。

【0083】引き続き、記憶サブシステムは手順1707において、得られたS\_IDをキーにして、図16の「WWN\_S\_ID\_GID変換テーブル」1601を検索し、このS\_IDに対応するGIDを取得する。ここまでの流れは、図19の手順1901、1902、1903の参照動作を指す。

【0084】手順1903において、当該S\_IDに対するGIDがテーブル1601で検索されない場合、当該ホストコンピュータにアクセス許可されたLUNはユーザによって登録されてなかったこととなり、当該ホストコンピュータからリクエストされたLUNへのアクセスは拒絶される。

【0085】続いて、手順1708（図17）において、このGIDに対してアクセス許可されているLUN情報を取得する。そして、手順1801（図18）において、このGIDをもつホストコンピュータのInquiryコマンドから得られたLUNが、「LUNアクセス管理テーブル」上でアクセス許可されたLUNとして登録されているか否かを判定する。ここまでの流れは、図19の手順1904および1905の参照動作を指す。

【0086】手順1904～1905における参照動作では、GIDをキーに、S\_IDからアクセス許可されたLUNを検索しているが、このGIDは個々のWWNをグループ化してまとめた属性であるため、一般に、GID：アクセス許可されるLUN＝多：1の関係となる。これは、従来のWWNをキーにしたLUNセキュリティのWWN：アクセス許可されるLUN＝1：1の関係よりも、ホストコンピュータ側の分解能が下がる分、検索動作が簡易になり一般に高速である。

【0087】「LUNアクセス管理テーブル」（図11、図12）の当該エントリに、手順1706で得られたLUNが登録されている場合、当該ホストコンピュータからそのLUNへのアクセスが許可されるため、記憶サブシステムは手順1802（図18）において、ホストコンピュータ応答用Inquiryデータのクオリファに2進数の'000'を、デバイスタイプに記憶サブシステムのデバイスタイプコードをセットする。

【0088】一方、「LUNアクセス管理テーブル」の当該エントリに、手順1706で得られたLUNが仮想LUNとして登録されていない場合、当該ホストコンピュータからその仮想LUNへのアクセスは拒絶されるため、記憶サブシステムは手順1803において、ホストコンピュータ応答用Inquiryデータのクオリファに2進数の'001'または、'011'を、デバイスタイプに16進数の'1F'をセットする。

【0089】次に記憶サブシステムは、手順1804において、FCP\_DATAフレームに上記の応答用Inquiryデータをセットして、ホストコンピュータへ送信する。続いて記憶サブシステムは、手順1805において、ホストコンピュータのInquiryコマンドの応答を完了したことを示すFCP\_RSPフレームを送信する。

【0090】図18の手順1802、1804に引き続いて、Inquiryデータを含むFCP\_DATAを記憶サブシステムから受信したホストコンピュータは、当該LUNへのアクセスは可能と判断し、以降、当該LUNへのアクセス可否を再度問い合わせることなく、アクセスを継続することができる。ここで、当該ホストコンピュータがアクセスするLUNは、実際にはLUNと一意に対応づけられた記憶サブシステム内の記憶領域#となる。

【0091】一方、手順1803、1804に引き続いて、Inquiryデータを含むFCP\_DATAを記憶サブシステムから受信したホストコンピュータは、当該LUNへのアクセスは不可能と判断し、以降、当該LUNへのアクセス可否を再度問い合わせることなく、アクセスもしない。

【0092】本実施例では、上記したようにホストコンピュータがアクセス可否を当該LUNへ問い合わせるのは、Inquiryコマンド発行時だけである。つまり、ログインが有効である間は、この問い合わせを繰り返し行う必要がない。これにより、ホストコンピュータと記憶サブシステム間のデータ転送効率を落とすことなく、強固なLUNセキュリティを実現できる。

【0093】尚、LUNから記憶サブシステム内の記憶領域#へのマッピングに「記憶領域#＝f(GID, LUN)」という相関関係をもたせた関数fとすれば、有効なGIDかつLUN値に対しては有効な記憶領域#が出力され、それ以外に対しては有効な記憶領域#が出力されないこととなる。

【0094】ここでf(n, m)は、GIDとLUNをパラメタに、ホストコンピュータに開示されたLUNを記憶サブシステム内の記憶領域#にマッピング変換する関数である。これにより、Inquiryコマンド以降のWriteコマンドやReadコマンドにおいて、手順1901～1905の検索動作を伴わずに、指定LUNから記憶領域#への変換動作中にアクセス可否チェックを最小限のオーバーヘッドで行うことができる。

【0095】以上のように、同一ポート配下で複数ホストコンピュータ群をグループ化して扱い、そのグループ単位にLUの割当てをユーザが任意に選択・設定可能な方法で実施することにより、ホストコンピュータ側の既存の処理、制限その他の機能を変えことなく、LUNセキュリティを高速な判定ロジックと記憶サブシステム内の記憶領域高効率使用と共に実現することができる。

【0096】本実施例では、ファイバチャネルを例に説明したが、実施においては、必ずしもファイバチャネルに限定する必要はなく、同等機能を提供可能なプロトコル環境であれば、その種別は問わない。また、記憶サブシステムに関しても、本実施例では、主にディスクアレイ装置を想定して記述しているが、通常の磁気ディスク装置や、記憶装置を媒体可換の光ディスクライブラリや、テープライブラリなどに置換することも可能である。

【0097】更には、最近のSAN環境の仮想化(Virtualization)を考慮して、本発明を複数の記憶サブシステム間で実施してもよい。この場合、前記の各テーブルの定義・設定事項は、1つの記憶サブシステム上で実施され、その他の記憶サブシステム内の論理ユニットに、その定義・設定が及ぶよう連絡通信経路を設け、1つの記憶サブシステムで集中して制御するよ

う構成する。

【0098】また、このような集中制御およびそれに必要なテーブルの定義は、必ずしも特定の記憶サブシステム上で行う必要はなく、複数の記憶サブシステムとFibreChannelその他共通インタフェースで接続され、複数の記憶サブシステム内の論理ユニットが認識可能であれば、ホストコンピュータ上のプログラム処理、またはスイッチング・ハブやルータ上の内部処理にもたせてもよい。このようにFibreChannel等のネットワークで結合された複数の記憶サブシステム間で本発明におけるLUNセキュリティを実現する場合では、アクセス許可された論理ユニットを内包した記憶サブシステム群と、ホストコンピュータ・グループと接続するポートをもつ記憶サブシステムやスイッチ、ルータは、同一筐体に属している必要はない。

【0099】

【発明の効果】コンピュータの既存の処理、制限その他の機能を変更せずに、記憶サブシステム内の管理テーブルを用いることによって、ユーザが任意にグループ化したホストコンピュータ群に、ユーザの運用希望に沿った形式で、記憶サブシステム内の論理ユニットを開示し、そのグループ単位で記憶サブシステム内のLUに対するアクセス可否を制限し、同時に、そのグループ単位に接続上のインターフェース設定が可能なセキュリティ機能を記憶サブシステムの単一ポート配下で提供することができる。

【0100】更に、記憶サブシステム内のLUに対するアクセス可否判定は、Inquiryコマンドのような問合せコマンド発行時点で判明するため、それ以降この判定を繰り返す必要がないため、記憶サブシステムを高い性能で維持運用しながら、LUに対する強固なセキュリティ機能を確保することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態におけるハードウェアの構成図である。

【図2】本発明の実施の形態におけるフレーム・フォーマットおよびそのフレーム・ヘッダの詳細を示す図である。

【図3】本発明の実施の形態におけるログインプロセスを示す図である。

【図4】本発明の実施の形態におけるInquiryコマンド送信時のフレーム・フォーマットの詳細を示す図である。

【図5】本発明の実施の形態におけるInquiryコマンドによる論理ユニットへのアクセス問合せシーケンスを示す図である。

【図6】本発明の実施の形態におけるLUNセキュリティの処理シーケンス概要を示すフローチャートである。

【図7】本発明を利用しないことによる不完全な「LUNアクセス管理テーブル」のフォーマットおよび、その第一の例を示す図である。

【図8】図7の状態を視覚的に示した図である。

【図9】本発明を利用しないことによる不完全な「LUNアクセス管理テーブル」のフォーマットおよび、その第2の例を示す図である。

【図10】図9の状態を視覚的に示した図である。

【図11】本発明の実施の形態における「LUNアクセス管理テーブル」のフォーマットおよび、その第一の利用例を示す図である。

【図12】本発明の実施の形態における「LUNアクセス管理テーブル」のフォーマットおよび、その第2の利用例を示す図である。

【図13】本発明の実施の形態におけるLUNセキュリティの効果を視覚的に示した図である。

【図14】本発明の実施の形態における「LUNアクセス管理テーブル」の作成シーケンスを示すフローチャートである。

【図15】本発明の実施の形態における「WWN\_S\_ID\_GID変換テーブル」の作成シーケンスを示すフローチャートである。

【図16】本発明の実施の形態における「WWN\_S\_ID\_GID変換テーブル」のフォーマットの第一の利用例を示す図である。

【図17】本発明の実施の形態におけるLUNセキュリティのホストコンピュータ送信のInquiryコマンドに対するLUNアクセス可否判定シーケンスを示すフローチャートである。

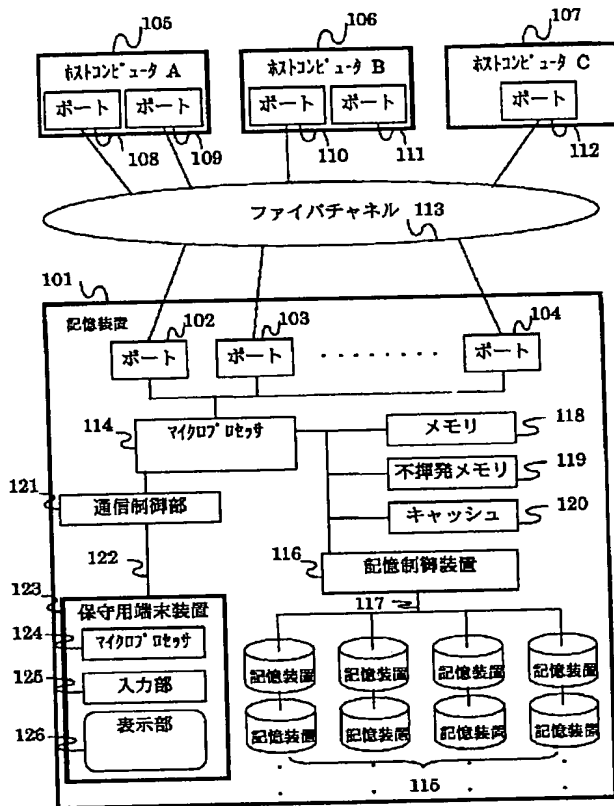
【図18】図17のフローチャートの続きを示すフローチャートである。

【図19】本発明の実施の形態におけるLUNセキュリティの各テーブル間の参照関係を示す図である。

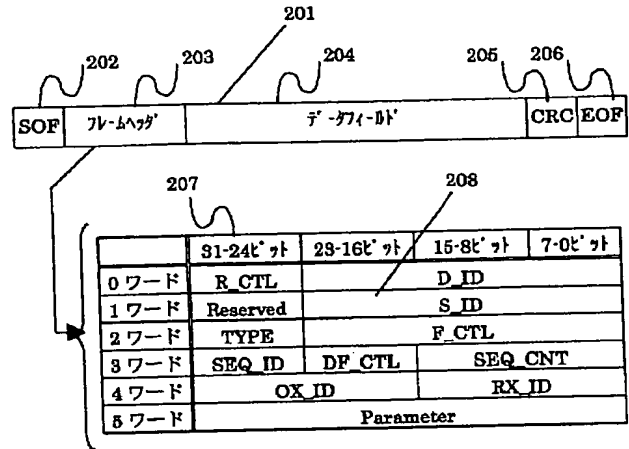
【符号の説明】

101……発明実施形態におけるハードウェア構成図、  
201……フレーム・フォーマット、207……フレーム・ヘッダの詳細、208……S\_ID、406……FCP\_CMNDフレーム・フォーマット、704……不完全な「LUNアクセス管理テーブル」の第1の例、801……記憶サブシステム、901……不完全な「LUNアクセス管理テーブル」の第2の例、1001……記憶サブシステム、1101……「LUNアクセス管理テーブル」の第1の例、1201……「LUNアクセス管理テーブル」の第2の例、1301……記憶サブシステム、1302……記憶サブシステムのポート配下に定義されたLU群LUA0~LUA4、LUB0~LUB2、LUC0~LUC3、1601……「WWN\_S\_ID\_GID変換テーブル」の第一の例。

【図1】



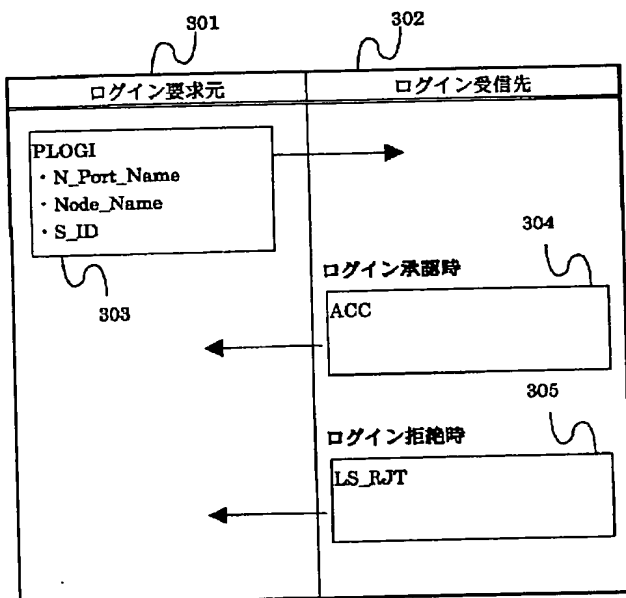
【図2】



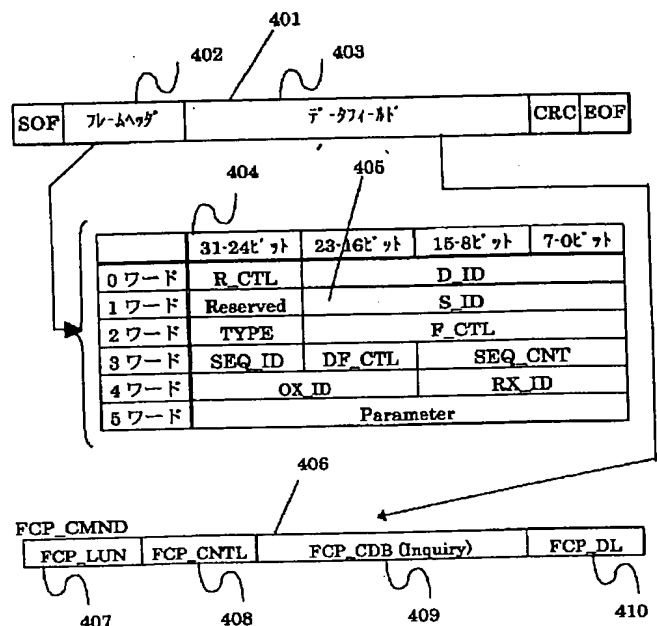
【図9】

WWN		LUN					
01234567	89ABCDAA	0	1	2	3	4	5
01234567	89ABCDAA0	6	7	8	9	10	
01234567	89ABCDAA1	11	12	13	14	15	

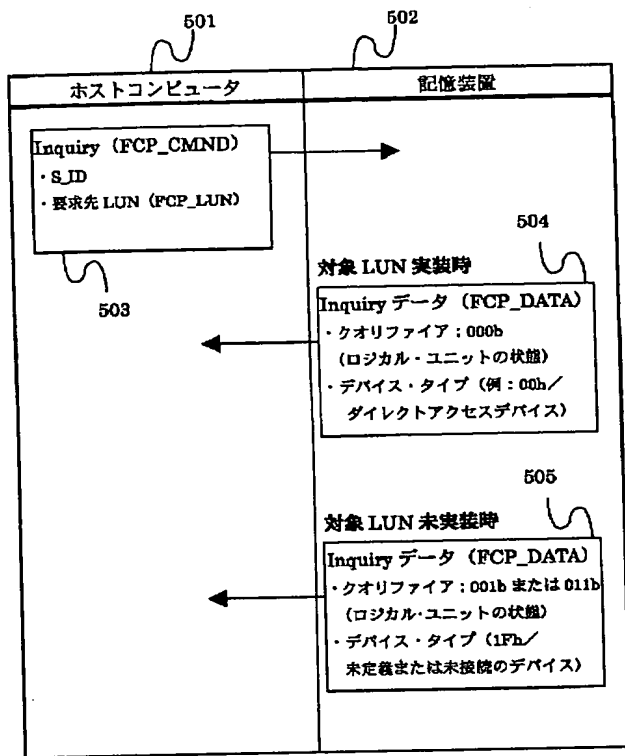
【図3】



【図4】



【図 5】



【図 7】

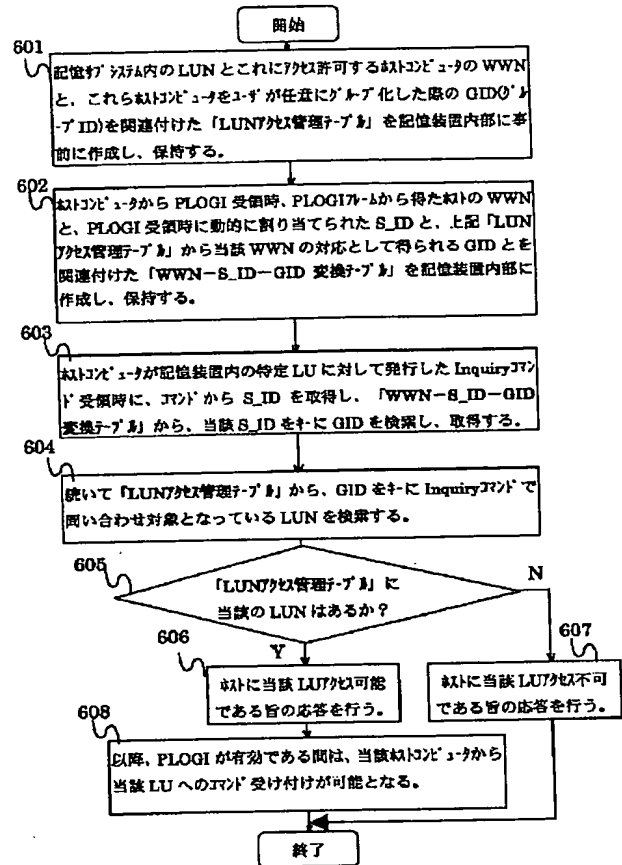
	WWN	LUN
702	01234567 89ABCDEF	0 1 2
703	01234567 89ABCDEE	3 4 7
704	01234567 89ABCDDE	5 6
705	...	...
706	01234567 89ABCDBB	0 1 7
707	01234567 89ABCDB0	3 5 6
708	01234567 89ABCDB1	2 4

【図 16】

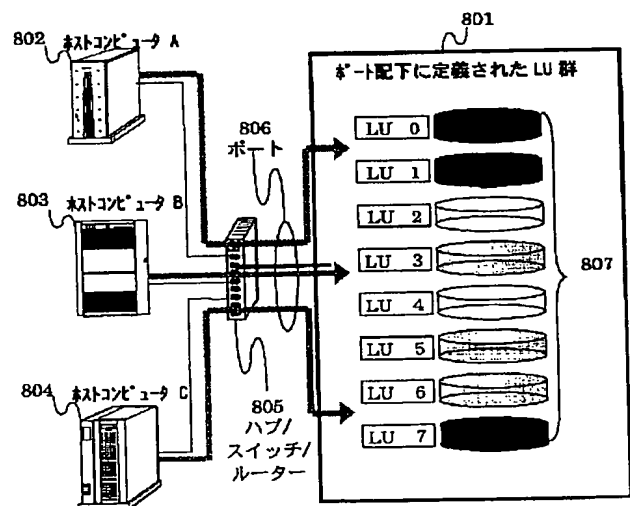
「WWN-S\_ID-GID 変換テーブル」

S_ID	WWN	GID
FFFF01	01234567 89ABCDEF	F001
FFFF02	01234567 89ABCDEE	F001
FFFF03	01234567 89ABCAAC	F002
FFFF04	01234567 89ABCAAD	F002
FFFF05	01234567 89ABCBA1	F0C1
FFFF06	01234567 89ABCBBE	F01F
FFFF07	01234567 89ABCDDE	F006
FFFF08	01234567 89ABCDCC	F006
...	...	...

【図 6】

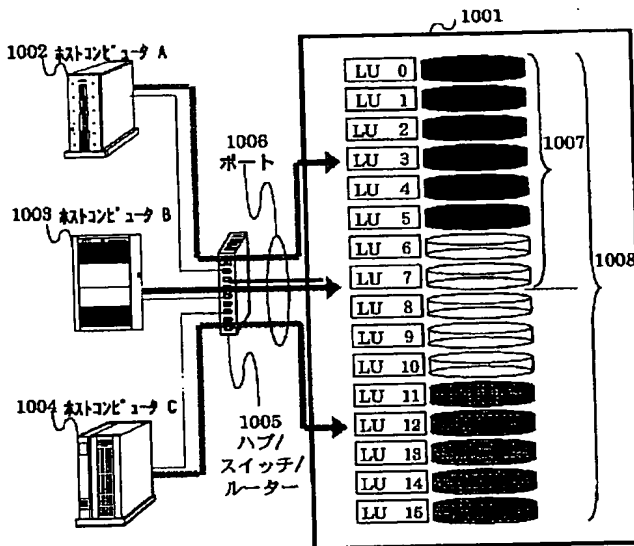


【図 8】





【図 10】



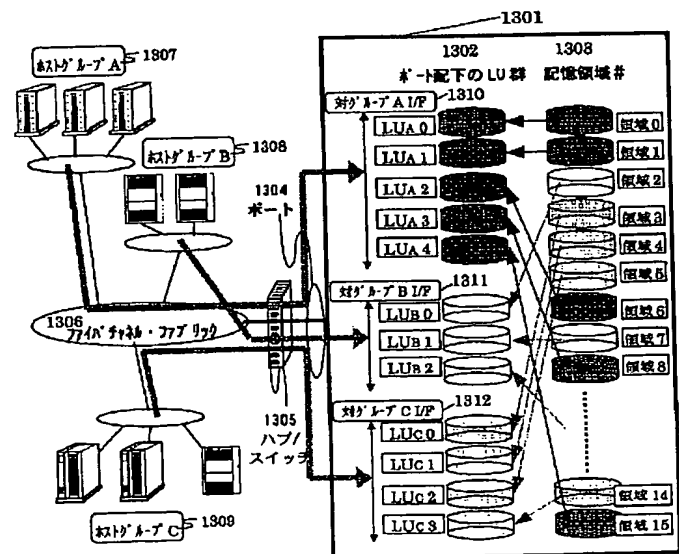
【図 11】

	GID	WWN	LUN
1105	Group A = F001 (OS 種 1)	1112 01234567 89ABCDEF 1113 01234567 89ABCDEE 1114 01234567 89ABCDEED	0 1 2 3 → 記憶領域「0 1 2 3」 を参照
1108	Group B = F002 (OS 種 2)	1115 01234567 89ABCDXX 1116 01234567 89ABCDYY 1117 01234567 89ABCDZZ	0 1 2 3 → 記憶領域 「60 61 62 63」を参照
1107	Group C = F003 (OS 種 3, 4 混在)	1118 01234567 89AB33DD 1119 01234567 89AB33CC 1120 01234567 89AB44BB 1121 01234567 89AB44AA	0 1 2 3 4 5 → 記憶領域 「7 11 70 79 87 119」 を参照
1108	Group D = F004 (OS 種 5, 6 混在)	1122 01234567 89ABCD10 1123 01234567 89ABCD2E	60 61 62 → 記憶領域 「40 90 100」を参照
1109	Group E = F005 (OS 種 1 の 1/2N)	1124 01234567 89ABCD81	0 1 → 記憶領域「4 5」参照
1110	Group F = F006 (OS 種 7)	1125 01234567 89ABCD46 1126 01234567 89ABCD4E	0 ~ 2 5 5 → 記憶領域「0 ~ 255」参照
1111	Group G = F007 (OS 種 7)	01234567 89ABCD46 01234567 89ABCD4E	0 ~ 2 5 5 → 記憶領域「256 ~ 512」参照
1127	Group H = F008 (OS 種 8 Floor 1)	1129 01234567 AAABCD46 1130 01234567 BBABCD4E	0 1 → 記憶領域「10 11」参照
1128	Group I = F009 (OS 種 8 Floor 2)	1131 01234567 CCABCD46 1132 01234567 DDABCD4E	4 5 → 記憶領域「10 11」参照

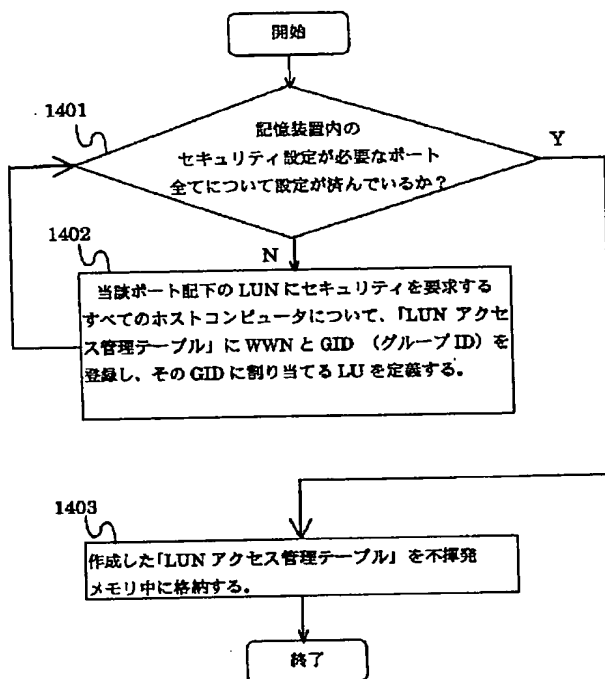
【図 12】

	GID	WWN	LUN
1205	Group A (GID=F001)	1208 01234567 89ABCAAC 1209 01234567 89ABCAA0 1210 01234567 89ABCA1	0 1 2 3 4
1206	Group B (GID=F002)	1211 01234567 89ABCBBE 1212 01234567 89ABCD8F	0 1 2
1207	Group C (GID=F003)	1213 01234567 89ABCDCC 1214 01234567 89ABCDCC 1215 01234567 89ABCDCC	0 1 2 3

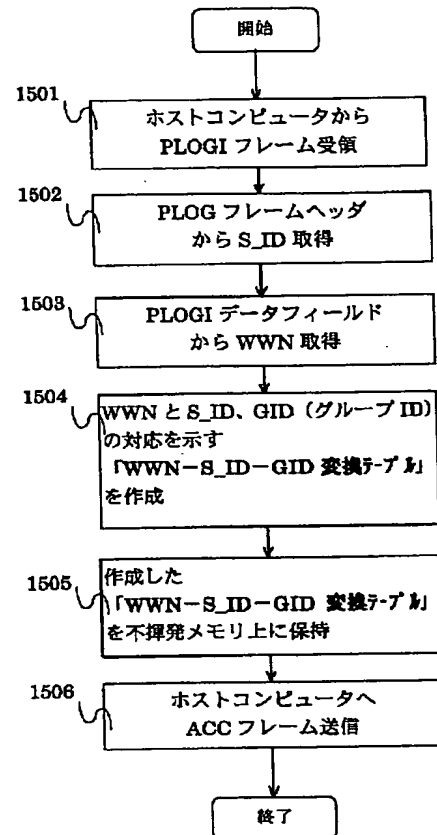
【図 13】



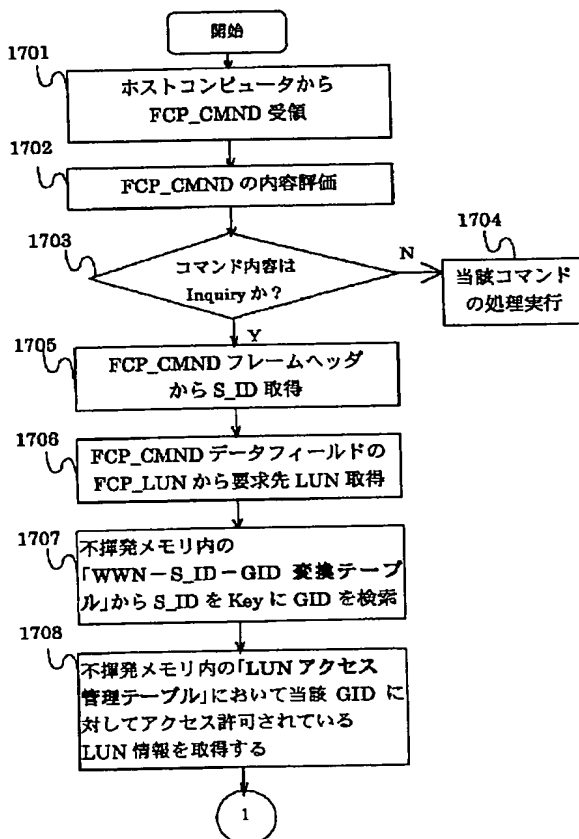
【図14】



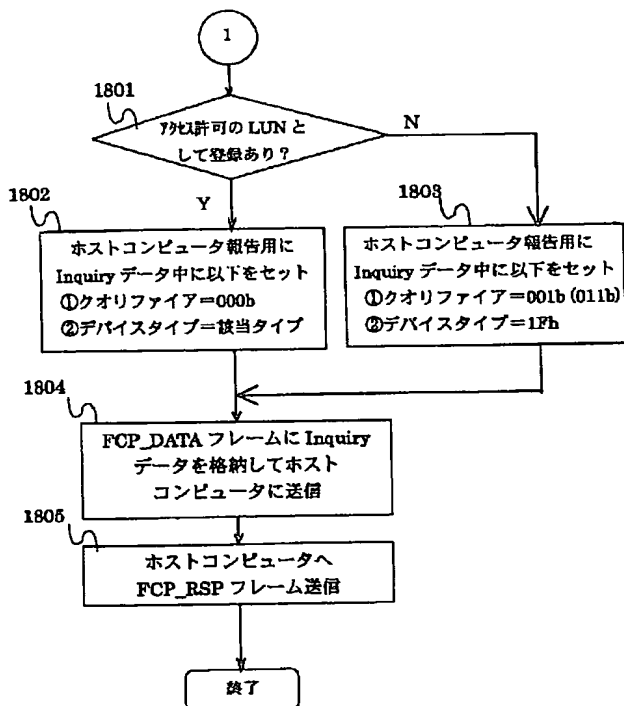
【図15】



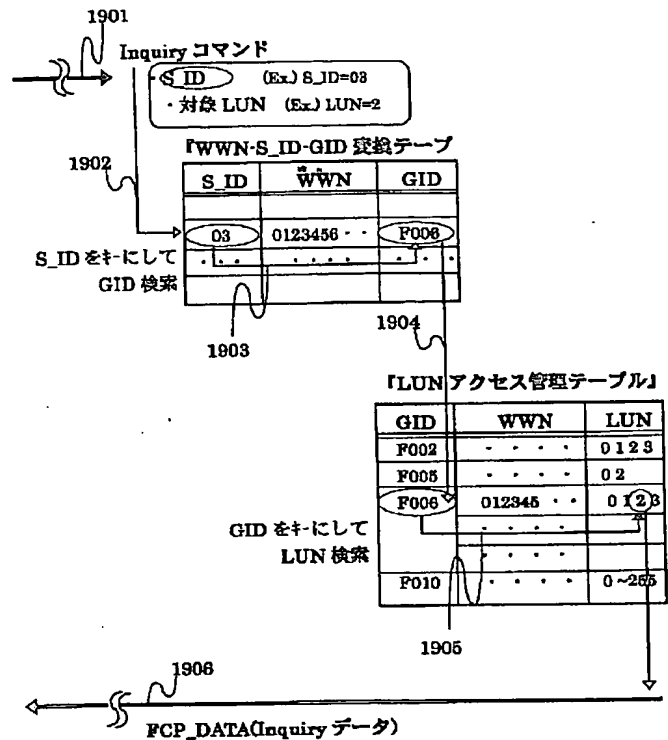
【図17】



【図 18】



【図 19】



フロントページの続き

(72) 発明者 内海 勝広  
神奈川県小田原市中里322番地 2 号 株式  
会社日立製作所 R A I D システム事業部内

(72) 発明者 五十嵐 良典  
神奈川県小田原市中里322番地 2 号 株式  
会社日立製作所 R A I D システム事業部内

(72) 発明者 堀 幸一  
神奈川県小田原市中里322番地 2 号 株式  
会社日立製作所 R A I D システム事業部内

F ターム (参考) 5B017 AA04 BA06 BB06 CA16  
5B065 BA01 CA02 CA11 PA13  
5B082 EA11 JA01